IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	C. A. No. 04-1199 (SLR) **Public Version**

SRI INTERNATIONAL, INC.'S RESPONSE TO DEFENDANTS' JOINT MOTION FOR SUMMARY JUDGMENT THAT SRI INTERNATIONAL, INC.'S PATENTS ARE INVALID FOR FAILURE TO DISCLOSE BEST MODE

Dated: June 30, 2006

FISH & RICHARDSON P.C.

John F. Horvath (#4557)
Kyle Wagner Compton (#4693)
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
FISH & RICHARDSON P.C.
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff and Counterclaim Defendant
SRI INTERNATIONAL, INC.

TABLE OF CONTENTS

TABLE OF CONTENTS (cont'd)

TABLE OF AUTHORITIES

Page

Cases

Statutes

I. INTRODUCTION

As the Defendants acknowledge, the patents-in-suit are directed to at least two novel concepts: (1) statistical intrusion detection on network data and (2) an analytical hierarchy of network monitors, both in the context of large-scale enterprise networks. These two central aspects of the inventions form their essence and represent marked innovations over earlier intrusion detection techniques. Yet the Defendants' motion accusing the inventors of failing to disclose the best mode of their invention focuses on two ***other*** aspects – a signature detection engine and receiving network data ("packet sniffing") – that were well-known in the art at the time of the filing of the patent and that are at most of secondary importance in the context of the claimed inventions.

Because the particulars of signature analysis and "packet-sniffing" amounted to mere implementation details, the inventors did not believe them to be essential components of the inventions and were therefore not obliged to append source code for those features to the specification. While the Defendants present ***argument*** to the contrary, the ***evidence*** establishes that the inventors did not subjectively consider specific signature analysis engines or packet-sniffing techniques to be the best modes of practicing any portions of their inventions. Moreover, they could not have so believed because these features were objectively tangential to the inventions. Furthermore, to the extent disclosure of either signature analysis or packet-sniffing was required, the inventors supplied sufficient detail in the specification. At a minimum, on the record before the Court, the Defendants cannot demonstrate the absence of material fact issues suitable for summary judgment of invalidity on the basis of best mode, a subjective and heavily factual inquiry. Accordingly, SRI respectfully requests that the Court deny the Defendants' motion.

II. STATEMENT OF FACTS

On one thing SRI and the Defendants agree: "there are two main facets to the claims of the patents-in-suit: (1) an analysis hierarchy of monitors; and (2) a statistical detection algorithm." [Op. Brief[1] at 3]. Through their research efforts, the inventors, Philip Porras and Alfonso Valdes, sought to expand and improve on already existing network intrusion detection techniques. [Porras Decl. ¶¶ 7-8]. One such conventional methodology, known as "signature analysis," compares network traffic to a library of known types of suspicious activity in order to determine whether the traffic in question is "undesirable." [*See* Moore Decl.[2], Ex. A at 7:25-27]. Signature analysis in general, and numerous particular signature-based algorithms, were well known in November 1998 when the patents-in-suit were filed. [Porras Decl.[3] ¶ 12; Ex. A[4] at 44, 46; Ex B at ¶¶ 138, 143, 147-48, 166, 168]. While useful for detecting known attacks, signature-based methodologies were vulnerable to new or stealthy intrusions. [*See* Porras Decl. ¶¶ 7-8]. Furthermore, because they required processing live network data against a large library of known suspicious activity, they operated at less than optimal speed. [*See id*].

Messrs. Porras and Valdes set out to improve these existing methodologies in two ways. First, they devised a statistical algorithm for examining network packet activity that might be suspicious but was not known to be malicious. [Porras Decl. ¶ 8]. This statistical technique built long-term profiles of normal network traffic and compared it against short-term activity. [*See* Moore Decl., Ex. A, all claims]. When it detected "anomalies" between the long-term and short-term profiles, the statistical engine could

---

[1] All references to "Op. Brief" denote the Defendants' Opening Brief in support of their Joint Motion for Summary Judgment That SRI International, Inc.'s Patents are Invalid For Failure to Disclose Best Mode. [D.I. 282].

[2] Moore Decl. refers to the Declaration of David E. Moore in Support of Defendants ISS and Symantec's Joint Motion for Summary Judgment that the Patents-in-Suit are Invalid for Failure to Disclose the Best Mode. [D.I. 284].

[3] "Porras Decl." refers to the Declaration of Phillip A. Porras in Support of SRI International Inc.'s Responses to Defendants' Motions for Summary Judgment, filed contemporaneously herewith.

determine that a potential attack–whether known or unknown–might be underway. [*Id.* at 2:30-34; 5-6]. The inventors developed an implementation of a statistical module following the principles of the invention known as eStat, whose source code they appended to the specification.

In addition, the inventors divided the labor of network monitoring among different levels of monitors in a "hierarchical" arrangement. [*See, e.g.*, Moore Decl., Ex. D, all claims]. Under this analysis hierarchy, network monitors process network traffic and pass reports of suspicious activity to higher-level monitors. [*Id.* at Col. 8]. This process enables much faster processing of network data, enables visibility of distributed suspicious activity, and operates largely without regard to the types of algorithms (statistical or signature-based) employed by the network monitors. [Porras Decl. ¶ 10].

In implementing their inventions in a real-world system, the inventors did ultimately develop their own signature analysis module, called expert, for use with their patented statistical analysis approach. [*Id.* at ¶ 12]. Additionally, they created an improved engine, known as etcpgen, for "packet sniffing" or receiving network data and grouping it into a useful form. [*Id.* at ¶ 25]. The etcpgen module was still under development at the time the patents-in-suit were filed. [Porras Decl. ¶ 27; *see infra*]. While signature analysis and packet-sniffing were well-known methodologies and formed only tangential portions of the invention, the specification of the patents-in-suit discloses how such techniques can be performed. [*See, e.g.*, Moore Decl., Ex. A at 5:7-8].

[4] Unless otherwise noted, all references to "Exhibits" denote exhibits to the Declaration of Kyle W. Compton in support of this brief, filed contemporaneously herein.

III. ARGUMENT

A. Legal standards

1. Summary judgment

Summary judgment is only appropriate where "there is no genuine issue as to any material fact and ... the moving party is entitled to a judgment as a matter of law." FED. R. CIV. P. 56(c). *See also Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 448 F.3d 1324, 1331 (Fed. Cir. 2006). All evidence presented by the non-movant is to be taken as true and all reasonable inferences must be drawn in the non-movant's favor. *Adickes v. S. H. Kress & Co.*, 398 U.S. 144, 157 (1970). Moreover, the appropriate level of proof required for a summary judgment motion is commensurate with the level of proof that would be required if the case went to trial. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 254-56 (1986) (requiring application of the "clear and convincing" standard to summary judgment motions in libel cases). Therefore, the Court cannot grant summary judgment of invalidity based on a failure to disclose the best mode without taking into account the Defendants' burden of clear and convincing evidence.

2. Patent validity under the best mode requirement

Patent law requires an inventor to set forth the best mode contemplated by the inventor for practicing his claimed invention. 35 U.S.C. § 112, ¶ 1 (2000). The presumption that a patent is valid requires an alleged infringer seeking to invalidate the patent based on the best mode to show by "clear and convincing evidence that the inventor both knew of and concealed a better mode of carrying out the claimed invention than that set forth in the specification." *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1330 (Fed. Cir. 2002). Thus, two underlying factual inquiries are required to determine compliance with the best mode requirement. *Intuitive Surgical, Inc. v.*

Computer Motion, Inc., 214 F. Supp. 2d 433, 443 (D. Del. 2002) (Robinson, C.J.) (denying motion for summary judgment because "due to the highly factual nature of this inquiry, the court declines to conclude, based on the record presented, that defendant has shown by clear and convincing evidence that the [patent-in-suit] is invalid for failure to disclose the best mode.") The first inquiry is wholly subjective while the second is largely objective. *Id.* (Citing *Chemcast Corp. v. Arco Indus. Corp.*, 913 F.2d 923, 927 (Fed. Cir. 1990)). The first prong considers "whether the inventor subjectively considered a particular mode of practicing the invention to be superior to all other modes at the time of filing the application", while the second prong examines "whether the inventor adequately disclosed that superior mode." *Teleflex*, 299 F.3d at 1330; *see also Dana Corp. v. IPC Ltd. P'ship*, 860 F.2d 415, 419 (Fed. Cir. 1988)[5] (best mode analysis "entails a comparison of the facts known to the inventor regarding the invention at the time the application was filed and the disclosure in the specification"). "[W]hether a best mode disclosure is adequate...is a function of not only what the inventor knew but also how one skilled in the art would have understood his disclosure." *Chemcast Corp. v. Arco Indus. Corp.*, 913 F.2d 923, 927 (Fed. Cir. 1990). An inventor need not disclose "routine details" apparent to one of skill in the art. *Liquid Dynamics Corp. v. Vaughan*

[5] Defendants cite *Dana Corp.* for the proposition that best mode can be determined as a matter of law and, implicitly, that summary judgment is appropriate in the best mode context. Yet the Federal Circuit in *Dana Corp.* did not review a summary judgment of best mode but rather a judgment notwithstanding the verdict and based its review "upon the evidence presented at trial." *Dana Corp.*, 860 F.2d at 419. In fact, it appears that in only a single published instance has the Federal Circuit affirmed a summary judgment of best mode, a case that Defendants cite for an entirely different proposition. *See U.S. Gypsum Co. v. National Gypsum Co.*, 74 F.3d 1209, 1212-13 (Fed. Cir. 1996). There, the inventor of a chemical compound explicitly admitted that a certain material was the best mode of practicing an invention. *Id.* at 1213. Yet he did not disclose the material in the specification – and indeed could not have done so – because its chemical composition and method of manufacture were trade secrets of

Co., 449 F.3d 1209, 2006 WL 1493004 (Fed. Cir. June 1, 2006). *See also Teleflex*, 299 F.3d at 1331-32.

B. The inventors disclosed the best mode of detecting suspicious network activity and had no obligation to furnish source code for expert in the '203, '615, and '212 patents

1. The inventors subjectively believed that statistical analysis and hierarchical monitoring – not signature techniques – formed the essence of their inventions

Under the first prong of the factual best mode inquiry, the court must examine the subjective views of the inventor. *Teleflex*, 299 F.3d at 1330; *Chemcast*, 913 F.2d at 927 (characterizing best mode inquiry as "a subjective, factual question."). Summary judgment is inappropriate if there is any evidence that casts doubt on whether the inventors subjectively considered a particular function to be the best mode as of the date they filed their application. [*See* Ex. C (*Optical Disc Corp. v. Del Mar Avionics*, 45 Fed. Appx. 887 (Fed. Cir. 2002)) at 895]. Because the subjective state of mind of the inventors is a question of fact, the Court must not weigh the relevant evidence on summary judgment and should instead focus wholly on whether the inventor admittedly knew at the time of filing his patent application of a method better than any other for practicing the claimed invention. *See Chemcast*, 913 F.2d at 927-28 ("Notwithstanding the mixed nature of the best mode inquiry, and perhaps because of our routine focus on its subjective portion, we have consistently treated the question as a whole as factual.")

At the time the patents-in-suit were filed, in November 1998, the inventors believed that statistical intrusion detection and hierarchical analysis formed the essence of the inventions. [Porras Decl. ¶ 7]. They considered statistical methodologies a potentially promising complement to signature analysis, which, as the Defendants' own

---

another company. *Id.* at 1213-14. Thus, not even Defendants claim that the rationale of *U.S. Gypsum* applies here.

experts have asserted, was well-known in the field at the time the patents-in-suit were filed. [*Id.* at ¶ 12; Ex. A at 44, 46; Ex. B at ¶¶ 138, 143, 147-48, 166, 168]. They also deemed the hierarchical aspects of the invention to be critical and they intended that the hierarchy would operate independently of the specific type of detection employed. [*Id.* at ¶ 10]. They further believed that any type of intrusion detection analysis technique–signature, statistical, or otherwise–could be used at any layer of the hierarchy.[6] [*Id.*] In short, the inventors simply did not consider their invention to be claiming signature-based analysis in general, let alone any specific type of signature engine. [*Id.* at ¶ 11].

The factual and testimonial record further confirms the inventors' subjective belief that the statistical engine and a hierarchical structure–not signature analysis–were the superior overall approach to detecting suspicious activity. As described in detail *infra*, the patents themselves are the clearest indication that signature-based techniques were tangential to the invention. The claims of the patents make clear that statistical and hierarchical analyses constituted the essence of the invention.

During their depositions, both Messrs. Porras and Valdes reaffirmed the importance of statistical analysis in general and the eStat engine in particular. In response to a question designed to elicit denigration of the eStat module, Mr. Porras expressly testified that eStat

REDACTED

[Ex. D at 235:20-21]. Mr. Valdes, who has spent the bulk of his career pursuing statistical intrusion detection, responded similarly to an argumentative question disparaging eStat by testifying that

REDACTED

[Ex. E at 495:12-20].

In many respects, the Defendants' own brief and exhibits themselves demonstrate the inventors' belief that the statistical and hierarchical aspects of the invention, not

[6] The claims of the '212 patent specifically require statistical analysis at the lowest level of the hierarchy.

anything related to signature analysis, formed its essence. In an ill-fated attempt to demonstrate the inventors' subjective belief of the importance of signature analysis and packet-sniffing, the Defendants cite portions of Messrs. Porras's and Valdes's testimony that establish precisely the opposite: the significance of statistical analysis and hierarchical monitoring. [*See* Op. Brief at 5

REDACTED

Time and again during their depositions, the inventors confirmed what the record plainly shows: the statistical and hierarchical facets of the patents-in-suit, not signature-based analysis or packet-sniffing, were their focus, and what they believed to be the core of their inventions.

The best that the Defendants can do to show the supposed importance of signature analysis is a single two-line snippet from an email message sent by Mr. Porras, describing the ability of the expert signature engine in the 1998 Lincoln Labs test to detect attacks that eStat, at that time, could not. [Moore Decl. Ex. P]. However, Mr. Porras observed just months later that the Lincoln Labs

REDACTED

[Ex. F]. For this reason, Mr. Porras believed at the time,

REDACTED

[*Id*]. In other words, Mr. Porras knew at the time that expert performed better in that specific Lincoln Labs test because the test was slanted in favor of a signature analysis approach rather than the statistical detection approach embodied in eStat. [*See also* Porras Decl. ¶ 17]. The email

does not say and cannot be fairly interpreted (especially on summary judgment) to say that the inventors believed expert to be better than eStat in the context of their inventions. [See Porras Decl. ¶¶ 15-17]. Mr. Porras confirmed that the Lincoln Labs results were not a meaningful indicator of the capability of eStat when he testified, in a portion not cited by the Defendants[7], that

REDACTED

[Ex. D at 235:22-25].

The Defendants further rely on a draft memorandum sent by Mr. Porras summarizing his preliminary hypotheses that certain well-known types of network attacks could be detected by a signature module like expert. [Moore Decl., Ex. L]. Mr. Porras introduced this memorandum – "Draft 0.1", dated just a few weeks before the patent was filed – by

REDACTED

Clearly that work had not been done yet, let alone progressed to the point where the inventors believed that either expert or etcpgen was the best way of practicing their inventions. [*See also* Porras Decl. ¶¶ 21-22].

In short, the inventors believed that statistical and hierarchical analysis represented the essence of their invention. Accordingly, they considered neither signature-based techniques nor the specific expert source code module to be the best mode of practicing their invention.

[7] Defendants' citation to deposition testimony is incomplete and misleading. The cited portions often do not even relate to, let alone support, the propositions for which they are cited; questions and portions of answers are frequently deleted; and entire pages of cited testimony are missing from the excerpts provided to the Court.

2. A signature engine *per se* was not claimed; to the extent one could be used to carry out a portion of the claimed invention, those of skill in the art knew how to do so

Even conceding that the inventors subjectively had a best mode, under the second prong of the factual best mode inquiry, the objective disclosure of the specification must be examined. *Intuitive*, 214 F. Supp. 2d at 443; *Teleflex*, 299 F.3d at 1330. However, the inventor need not disclose (1) subject matter known to the inventor but outside the claimed portions of the invention; and (2) "routine details" which are apparent to one of skill in the art. *Cardiac Pacemakers, Inc. v. St. Jude Med., Inc.*, 381 F.3d 1371, 1379 (Fed. Cir. 2004) (finding no invalidity for failure to disclose the type of battery used even though the claimed invention needed some type of battery to function); *Teleflex*, 299 F.3d at 1330.

First, the best mode requirement applies to the claimed subject matter alone. *Cardiac Pacemakers*, 381 F.3d at 1379; *see also Randomex, Inc. v. Scopus Corp.*, 849 F.2d 585, 588-90 (Fed. Cir. 1988) (finding no invalidity where a generic cleaning solution was disclosed over a more efficient cleaning solution the inventors used because the invention neither "added nor claimed to add anything to the prior art respecting cleaning fluid."); *Engel Indus., Inc. v. Lockformer Co.*, 946 F.2d 1528, 1532 (Fed. Cir. 1991) ("The best mode inquiry is directed to what the applicant regards as the invention, which in turn is measured by the claims."); *Eaton Corp. v. Parker-Hannifin Corp.*, 2003 WL 252154, at *1-2 (D. Del. Jan 28, 2003) (Robinson, C.J.) (denying summary judgment of invalidity for failure to recite best mode upon reconsideration when defendant could not demonstrate "where in the claims" the feature in question appeared). The reason for limiting the inquiry to the claimed invention is "pragmatic: the disclosure would be boundless and the pitfalls endless." *Engel Indus.*, 946 F.2d at 1531. A violation of the

best mode requirement may exist where subject matter not strictly within the claim boundaries is concealed, but only when "the alleged best mode information bore a strong relationship to the claimed invention or implicated questions of concealment." *Teleflex*, 299 F.3d at 1331 (collecting cases and identifying the "critical" or "necessary" aspect of the unclaimed element).

Second, inventors may omit "production details" or "routine details." *Teleflex*, 299 F.3d at 1331-32. Even routine details that "*do* relate to the quality or nature of the invention" do not need to be disclosed unless they "would not have been apparent to one of ordinary skill in the art." *Young Dental Mfg. Co. v. Q3 Special Prods., Inc.*, 112 F.3d 1137, 1144 (Fed. Cir. 1997) (emphasis in original); *see also Eli Lilly & Co. v. Barr Labs., Inc.*, 251 F.3d 955, 966 (Fed. Cir. 2001) (finding selection of a particular solvent to be a routine detail and not requiring disclosure of the particular type of solvent the inventor used).

Here, specific signature-based techniques are not claimed; to the extent signature-based methodologies are mentioned in the patents, persons of skill in the art knew how to perform them at the time of filing. Instead, the novelty of the '212, '203, and '615 patents derives primarily from the claimed hierarchical analysis structure. This component, and the improvement in detection capabilities it provides, furnishes the innovative aspect of the invention, as the Defendants readily acknowledge. [Op. Brief at 3]. The particular techniques implemented at any level of that hierarchy – including the use of a signature engine – are unclaimed details that alone impart no novelty to the invention. The use of a signature engine, whether expert or some other algorithm, is akin to the batteries recited in the claims of the *Cardiac Pacemakers* patents or the cleaning fluid in *Randomex*: the details of the signature engine in use make no difference because

the invention is "not about" signature analysis. *See Cardiac Pacemakers*, 381 F.3d at 1379; *see also Randomex*, 849 F.2d at 588-90.

a. The '212 patent is directed to statistical analysis and hierarchical monitoring

The claims of the '212 patent are explicitly directed to statistical analysis and hierarchical monitoring. Both independent claims – 1 and 14 – center around a "statistical detection method" and "hierarchical monitors", thus rendering thoroughly implausible the Defendants' argument that signature analysis constituted the best mode. Instead, a "signature matching detection method" is discussed only in two ***dependent*** claims, with no particular details required, underscoring the relative insignificance of signature analysis in the context of the invention. As such, there was no reason to include source code for expert, a specific signature analysis engine, in the specification. *See Cardiac Pacemakers*, 381 F.3d at 1379; *Engel Indus.*, 946 F.2d at 1532 ("The best mode inquiry is directed to what the applicant regards as the invention, which in turn is measured by the claims.").

b. The '203 and '615 patents are directed to hierarchical monitoring

The claims of the '203 and '615 patents likewise are not about signature analysis. The independent claims of these patents focus on "hierarchical event monitoring and analysis" in the method claims and "hierarchical monitors" in the apparatus claims. In ***none*** of the claims in these patents is signature analysis even mentioned. *See Eaton Corp.*, 2003 WL 252154, at *1-2. Thus, again, the inventors would have had no reason to include the expert source code in the specification. *See Cardiac Pacemakers*, 381 F.3d at 1379; *Engel Indus.*, 946 F.2d at 1532.

Furthermore, signature engines were well-known in the art at the time of the filing of the patents-in-suit. [Porras Decl. ¶ 12]. The Defendants' own experts repeatedly opine to this effect. [Ex. A at 44, 46; Ex. B at ¶¶ 138, 143, 147-48, 166, 168]. Signature engines are relevant to the inventions only insofar as they constitute part of the novel

hierarchy of network monitors and serve as an adjunct to the novel statistical engine. [*See* Porras Decl. ¶ 10].

The Defendants' attempt to tie the alleged requirement for disclosing the details of a specific signature analysis module to the claim language of "detecting suspicious network activity" is particularly disingenuous, given that one of their own experts is adamant that signature engines ***do not*** detect suspicious activity. ISS's expert, Stephen Smaha, opined that ISS's Protocol Analysis Module ("PAM"), one of the accused products he characterized as a signature-based engine, was not

REDACTED

[*Id.*] This directly contradicts the argument in the Defendants' present motion.

The Defendants in their brief also criticize the inventors for not including in the patents specific signatures for detecting "SYN flood" attacks. Here again, Mr. Smaha explicitly described SYN floods as "not 'suspicious.'" [Op. Brief at 7-8 & n.6; Ex. G at 8]. If Mr. Smaha believes that signature engines do not detect suspicious network activity in general – and SYN floods in particular – the Defendants cannot possibly fault SRI for failing to include source code for such engines in a patent directed to detecting suspicious network activity. [*Cf.* Op. Brief at 4 ("the signature-based analysis unit can be used for *detecting suspicious network activity*.")] and at 3 n.2 ("Signature detection entails comparing monitored activity to known patterns of suspicious activity.") *with* Ex. G at 8. REDACTED The Defendants' multiple and self-contradictory positions on whether signature engines detect suspicious network activity, alone, preclude entry of summary judgment. At the very least, it is clear that signature-based analysis objectively constituted an insignificant part of SRI's inventions directed to detecting suspicious network activity.

In short, the patents-in-suit "neither added nor claimed to add anything to the prior art respecting" the particulars of signature-based detection. *Randomex*, 849 F.2d at 590. There was therefore no need to disclose any source code for routine details like signature analysis, which at the time was widely understood by those of skill in the art. *See Teleflex*, 299 F.3d at 1331-32; *Young Dental*, 112 F.3d at 1144; *Chemcast*, 913 F.2d at 927.

3. Even if the signature engine *was* an essential part of the claimed invention, it was disclosed in the specification

"As a general rule, where software constitutes part of a best mode of carrying out an invention, description of such a best mode is satisfied by a disclosure of the functions of the software." *Fonar Corp. v. Gen. Elec. Co.*, 107 F.3d 1543, 1549 (Fed. Cir. 1997). "[W]hen disclosure of software is required, it is generally sufficient if the functions of the software are disclosed, it usually being the case that creation of the specific source code is within the skill of the art." *Robotic Vision Sys., Inc. v. View Engineering, Inc.*, 112 F.3d 1163, 1166 (Fed. Cir. 1997) (citing *Fonar*); *see also Zumbro, Inc. v. Merck & Co.*, 819 F. Supp. 1387, 1403 (N.D. Ill. 1993) ("Computer programs need not always be disclosed to fulfill the best mode requirement; if the patent furnishes the information necessary to write such programs, there would seem to be no cogent reason to require disclosure of the menial tools known to all who practice this art." (internal quotations omitted)). So long as the specification "delineates the best mode in a manner sufficient to require only the application of routine skill to produce a workable digital computer program" then the requirement will be met. *In re Hayes Microcomputer Prods. Inc. Patent Litig.*, 982 F.2d 1527, 1537 (Fed. Cir. 1992). Stated another way, if the specification provides sufficient detail for a skilled programmer to act in a mere "clerical

function" then the best mode requirement is met. *In re Sherwood*, 613 F.2d 809, 817 (C.C.P.A. 1980).

To the extent that signature analysis constituted part of the invention claimed in the '212, '203, and '615 patents[8], the inventors disclosed its critical functions in the specification. *See Fonar*, 107 F.3d at 1549. The patent devotes nearly a full column to a detailed description of how the signature engine may operate and provides another column of disclosure on how a "resolver" can settle discrepancies between the signature and statistical analysis modules. [Moore Decl., Ex. A[9] at 7:24-8:13; 8:14- 9:7].

Specifically, the specification defines the signature engine as an element that "maps an event stream against abstract representations of event sequences that are known to indicate undesirable activity." [*Id.* at 7:24-26]. The patent explains that signature analysis can be performed at multiple levels of the analytical hierarchy. [*Id.* at 7:26-29]. Its functions include scanning "the event stream for events that represent attempted exploitations of known attacks against the service" and scanning "the aggregate of intrusion reports from service monitors in an attempt to detect more global coordinated attack scenarios." [*Id.* at 7:31-37].

The specification details typical types of attacks that the signature engine can detect, including "address spoofing, tunneling, source routing, SATAN attacks, and abuse of ICMP messages." [*Id.* at 7:43-45]. One such method of analysis set forth in detail is "threshold analysis", which detects and indicates when the number of a certain kind of inherently suspicious event – seven examples of which are listed – "surpasses a reasonable count." [*Id.* at 7:46-50]. Such thresholds can be set for the number of fingers, pings, or failed login requests to certain types of accounts. [*Id.* at 7:51-54].

[8] Again, the only place that the claims even mention signature analysis is in two dependent claims in the '212 patent.
[9] The specification for all of the patents-in-suit is largely identical.

The patent further recites that the signature engine can "examine the data portion of packets in search of a variety of transactions that indicate suspicious, if not malicious, intentions by an external client." [*Id.* at 7:55-57]. Such an analysis can be performed on FTP, HTTP, or Gopher traffic and can detect "anonymous requests to access non-public portions of the directory structure." [*Id.* at 7:58-62]. The signature engine can also "scan traffic directed at unused ports" in an effort to discover "network services that have been installed without an administrator's knowledge." [*Id.* at 8:1-13]. The specification then proceeds to explain how the resolver may handle suspicious activity reports submitted by both the signature analysis module and the statistical engine. [*Id.* at 8:14-9:7].

Thus, the patent more than adequately lays out the key functions of a signature analysis component, were one to be used. *See Fonar*, 107 F.3d at 1549. This disclosure would easily have enabled the creation of corresponding source code through mere "application of routine skill". *In re Hayes*, 982 F.2d at 1537. Even had signature engines not been widely known in the art when the '338 patent was filed, there was no need for the inventors to disclose ***any*** source code, since creation of the code was well within the skill of the art at the time. *Robotic Vision Sys.*, 112 F.3d at 1166. As such, the inventors satisfied the best mode requirement. Accordingly, the Defendants' motion should be denied.

C. The inventors did not believe etcpgen was the best mode of receiving network packets handled by a network entity at the time they filed their application, did disclose adequate detail about how to receive network packets in general, and therefore had no obligation to furnish source code for etcpgen in the '338 patent

One of the more rudimentary processes in intrusion detection involves receiving network packets, selecting relevant portions therefrom, and grouping the data into an "cvent", a process known informally as "packet-sniffing." At the time of the invention, packet-sniffing was a routine, well-understood procedure, as the Defendants' own experts acknowledge. Yet the Defendants wrongly contend that the inventors should have included source code for one specific packet-sniffing engine, known as etcpgen, in the

application for the '338 patent. The inventors did not believe that the best mode for carrying out the invention involved any particular packet-sniffing methodology. Moreover, at the time of the filing of the patents-in-suit, they had not finished developing the etcpgen engine. Furthermore, packet-sniffing was an insignificant component of the '338 patent, which is directed purely to an innovative statistical analysis technique. To the extent that packet-sniffing was relevant to the invention, the inventors duly described its functionality in the specification.

1. The inventors did not subjectively believe that etcpgen was an essential part of the claimed invention or the best mode of "receiving network packets" as it was still under development at the time the '338 patent was filed

The inventors did not believe that etcpgen formed any significant part of the invention. [Porras Decl. ¶ 24]. During the time that the '338 patent was filed, numerous packet-sniffing techniques were known to the public. [*Id.* at ¶ 23; *see also* Ex. A at 30]. It was unclear to the inventors which if any of these approaches was preferable in the context of their invention. [Porras Decl. ¶ 26]. Development simply had not proceeded far enough at that time for such a determination to be made. [*Id.* at ¶ 27].

During his deposition, Mr. Porras confirmed this chronology, stating that

REDACTED

[*Id.* at 173:21-174:1].

Even December 1998, of course, is after the filing of the '338 patent. The Defendants' citation to this portion of Mr. Porras' transcript even undermines their contention that etcpgen represented the best mode of packet-sniffing at the time of the filing of the '338 patent: in response to a question of

REDACTED

[*Id.* at 174:4-11 (emphasis added)]. In other

words, only ***after*** the patents-in-suit were filed did etcpgen emerge as a superior mechanism for selecting and aggregating network traffic data.

Contemporaneous documentation further establishes that etcpgen was still in development around the time of the filing of the patents-in-suit. In the draft EMERALD expert/estat summary distributed on October 16, 1998, Mr. Porras describes the development status of the etcpgen module. He refers to REDACTED an indication that this particular engine for generating events from network packets was still a work in progress less than four weeks before the filing of the patents-in-suit. [Moore Decl., Ex. L at SRIE_0277991-992]. Mr. Porras also asked Martin Fong, the engineer assigned to handle development of etcpgen, to configure the program to format data packets in a particular way and to ignore packets ***not*** formatted in that way. [*Id*]. Thus, the etcpgen module was still in development around the time that the '338 patent was filed. The inventors therefore could not have considered etcpgen to be the best mode at that time.

2. Packet-sniffing was not an essential part of the claimed invention and was widely known in the field at the time the '338 patent was filed

The '338 patent is directed to statistical methods of network intrusion detection. All of the independent claims center on building long-term and short-term statistical profiles from the network traffic passing through a "network entity." While the independent claims also contain the phrase "receiving network packets", this routine, widely-known process does not constitute a novel or significant component of the invention. [Porras Decl. ¶¶ 23-24].

As discussed above, numerous techniques for receiving and grouping network traffic data were known to the public as of November 1998. [Porras Decl. ¶ 23]. One of Defendant ISS's own experts, Stephen Smaha – citing one of Defendant Symantec's experts, Todd Heberlein – testified precisely to this effect, stating in his expert report on invalidity that REDACTED

REDACTED

[Ex. A at 30]. Mr. Smaha discussed a product known as Sniffer, which he claimed was created before 1990, and pointed to deposition testimony by one of SRI's employees that similar technology was relatively common in 1997. [*Id.* (citing Lunt Tr. at 229:16-18)]. Mr. Smaha went on to describe REDACTED available to and known in 1998. [*Id.* at 30-31]. Mr. Smaha's report thus further underscores the availability of a diversity of techniques for packet-sniffing at the time the '338 patent was filed.

Therefore, not surprisingly, the '338 patent "neither added nor claimed to add anything to the prior art respecting" methodologies for receiving and grouping network data. *Randomex*, 849 F.2d at 590. Furthermore, one of skill in the art as of November 1998 would clearly have understood the inventors' disclosure sufficiently with regard to packet-sniffing, as the Defendants' experts acknowledge. *See Teleflex*, 299 F.3d at 1331-32; *Young Dental*, 112 F.3d at 1144; *Chemcast*, 913 F.2d at 927. Accordingly, the Court should deny the Defendants' motion.

3. To the extent that packet-sniffing *was* part of the claimed invention, it was disclosed in the specification

To the extent that generating events from packet data constituted part of the invention claimed in the '338 patent, the inventors disclosed its critical functionality in the specification. *See Fonar*, 107 F.3d at 1549. Both of the major components of packet-sniffing – namely, techniques for selecting packets and for aggregating packet data into an event – are described in detail in various portions of the patent.

First, the specification states that:

> [s]election of packets can be based on different criteria. Streams of event records can be derived from discarded traffic..., pass-through traffic..., packets having a common protocol..., packets involving network connection management (e.g., SYN, RESET, ACK...), and packets targeting ports to which an administrator has not assigned any network service...

[Moore Decl, Ex. A. at 5:4-14]. The specification goes on to recite that "[e]vent streams may also be based on packet source addresses...or destination addresses" and that "[s]election can also implement application-layer monitoring..." [*Id.* at 5:15-21]. Furthermore, it states that "[e]vent streams can be of very fine granularity. For example, a different stream might be derived from commands received from different commercial web-browsers..." [*Id.* at 5:25-27]. Thus, the patent sets forth the critical details involved in selecting packets, as conceded by the Defendants. [Op. Brief at 5 ("the patent lists various criteria for selecting packets")].

Second, the specification states that "[a] monitor 16 can also construct interval summary event records, which contain accumulated network traffic statistics (e.g., number of packets and number of kilobytes transferred)." [*Id.* at 5:30-33]. It then describes the frequency of when such events are constructed, reciting that "[t]hese event records are constructed at the end of each interval (e.g., once per N seconds)." [*Id.* at 5:30-35]. The patent goes on to detail how these events are processed, stating that "[e]vent records are forwarded to the analysis engines 22, 24 for analysis." [*Id.* at 5:35-36]. The specification therefore explains how events are constructed from selected packets.

Thus, the patent more than adequately lays out the functions of packet-sniffing software. *See Fonar*, 107 F.3d at 1549. This disclosure would easily have enabled the creation of relevant source code through mere "application of routine skill". *In re Hayes*, 982 F.2d at 1537. There was no need for the inventors to disclose ***any*** source code, since creation of the code was within the skill of the art at the time. *Robotic Vision Sys.*, 112 F.3d at 1166. Accordingly, the inventors satisfied the best mode requirement. For this reason as well, the Defendants' motion should be denied.

D. SRI has consistently rebutted the Defendants' speculative best mode defense

As amply demonstrated above, both the factual record and the deposition testimony reveal that the inventors disclosed the best mode of detecting suspicious network activity. Even in the face of hostile questioning at their depositions, the inventors steadfastly reiterated the importance of statistical and hierarchical analysis and the corresponding insignificance of the signature engine and packet-sniffing details of the invention. The record is replete with evidence countering the Defendants' best mode assertions.

Yet the Defendants insist – without supporting citation – that SRI has not adequately rebutted their best mode defense in its "responsive contention interrogatories." [Op. Brief at 16]. While the Defendants do not define this phrase, they are presumably referring to Defendant ISS's Supplemental Responses to SRI's Interrogatories Nos. 6. In the first of these, served on November 15, 2005, ISS asserted:

> The claims-at-issue are also invalid under 35 U.S.C. § 112 for failure to satisfy the best mode requirement. SRI submitted source code in an Appendix to the patents-in-suit. A preliminary examination of that code indicates that it is not a complete program and could not compile and run. The Appendix appears to lack configuration files that would relate specifically to network traffic data or analysis. The code also does not have code for a resolver. On information and belief, ISS believes discovery will show that SRI had a more complete set of source code by the time it filed U.S. Patent Application No. 09/188,739 and withheld much of that code from the Patent Office. That withheld code reflected the inventor's best mode of practicing the claims at issue.

[Ex. H at 9]. ISS alleged that the source code attached to the specification was lacking in three ways: (1) it was incomplete and could not compile and run; (2) it lacked configuration files relating to "network traffic data or analysis"; and (3) it did not contain code for a resolver. These contentions were both untrue and ambiguous at the time they were served and they remain so now. More importantly, the Defendants' current motion is predicated on none of these three supposed deficiencies. Therefore, SRI had no

obligation to rebut the different allegations on which the Defendants now rely to make their best mode argument.

As for the Defendants' now-abandoned best mode allegations, SRI ***did*** respond. On November 15, 2005, the same day ISS served the supplemental response excerpted above, ISS propounded an interrogatory asking SRI to explain "why each ground presented in ISS's Supplemental Response to Interrogatory [sic] No. 6 does not render the claims of the patents-in-suit invalid." [Ex. I at 2]. In response, on December 15, 2005, SRI stated:

> Defendants' contention that the claims-at-issue are invalid for failure to satisfy the best mode requirement under 35 U.S.C. § 112 is based solely on speculation. The Defendants have failed to identify any evidence that the inventors did not provide the U.S. Patent Office with the most complete source code they believed was available to them as of November 9, 1998. Defendants fail to disclose any other particular contention regarding other basis for invalidity under 35 U.S.C. 5 112 in a manner sufficient for SRI to respond.

[Ex. J at 50].

On January 19, 2006, Symantec served a supplemental response to SRI's Interrogatory No. 6, asserting in language almost identical to that of ISS that:

> The claims-at-issue are also invalid for failure to satisfy the best mode requirement under 35 U.S.C. § 112. SRI submitted source code in an Appendix to the patents-in-suit. A preliminary examination of the source code provided in the Appendix indicates that the code in the Appendix is not the complete program that existed at the time. For example, the Appendix code would not compile and run. In addition, the Appendix code contains no configuration files allowing for the use of any particular network traffic data categories. Furthermore, the Appendix code does not appear to have code for a resolver or an expert system. On information and belief, Symantec believes discovery will show that SRI had a more complete set of source code by the time it filed U.S. Patent Application No. 09/188,739 and withheld much of that code from the Patent Office. That withheld code reflected the inventor's best mode of practicing the claims-at-issue.

[Ex. K at 10-11]. Again, there is nothing in this response that resembles what the Defendants now say is the basis for their best mode defense. And unlike ISS, Symantec

never even served an interrogatory asking SRI to respond to these contentions, so Symantec has no basis at all for making a preclusion argument.

On April 10, 2006, ISS served a second supplemental response to Interrogatory No. 6 in which it reiterated its earlier belief that the inventors failed to disclose the best mode of carrying out their invention. These allegations were similarly general and ambiguous; ISS contended only that source code "pertain[ing] to SRI's best known mode of practicing the Asserted Claims...was withheld from the Appendix submitted to the Patent Office." [Ex. L at 10]. As evidence of these assertions, ISS generally referred, without citation, to the deposition of five SRI employees and to nearly 40 responses to requests for admission. [*Id.* at 10-11]. Symantec never updated its interrogatory response with respect to its best mode defense. SRI stood on its denial of ISS's vague and unspecified allegations. Only during expert discovery did the Defendants clarify the basis for their best mode assertions, a basis that the factual and testimonial record amply refutes.

In addition, the Defendants disparage SRI because its liability expert, Dr. George Kesidis, did not rebut any of their purported best mode arguments. However, technical experts are not in any position to opine on the inventors' ***subjective intent*** during the filing of the patents-in-suit. [Ex. M at 302:17-19

REDACTED

Even if Dr. Kesidis had spoken with the inventors about their subjective beliefs, any testimony he might have provided would not have added anything to the evidentiary record.

Regardless, during his deposition, Dr. Kesidis ***did*** furnish testimony that reaffirmed the basis for the reasons, described above, that the inventors would not have been obligated to disclose expert or etcpgen. Dr. Kesidis indicated that there was considerable uncertainty concerning whether

REDACTED at the time the patents-in-suit were filed. [*Id.* at 301:25-

302:5]. He further testified that he believed

REDACTED

[*Id.* at 307:5-10]. In other words, Dr. Kesidis confirmed several key aspects of the factual and testimonial record, namely that eStat was the best available analysis module and that expert – which figured prominently in the inconclusive Lincoln Labs testing – was not.

Accordingly, the inventors, SRI, and SRI's expert more than adequately rebutted the Defendants' best mode defense.

IV. CONCLUSION

For the foregoing reasons, SRI respectfully requests that the Court deny the Defendants' motion.

Dated: June 30, 2006

FISH & RICHARDSON P.C.

By: */s/ John F. Horvath*

John F. Horvath (#4557)
Kyle Wagner Compton (#4693)
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff/Counterclaim Defendant
SRI INTERNATIONAL, INC.

50355813.doc

CERTIFICATE OF SERVICE

I hereby certify that on July 10, 2006, I electronically filed the **REDACTED –SRI INTERNATIONAL, INC.'S RESPONSE TO DEFENDANTS' JOINT MOTION FOR SUMMARY JUDGMENT THAT SRI INTERNATIONAL, INC.'S PATENTS ARE INVALID FOR FAILURE TO DISCLOSE BEST MODE** with the Clerk of Court the attached document using CM/ECF which will send electronic notification of such filing(s) to the following Delaware counsel.

Richard L. Horwitz
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
P.O. Box 951
Wilmington, DE 19899

Attorneys for Defendant-Counterclaimant Internet Security Systems, Inc., a Delaware corporation, and Internet Security Systems, Inc., a Georgia corporation

Richard K. Herrmann
Morris James Hitchens & Williams
PNC Bank Center
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306

Attorneys for Defendant-Counterclaimant Symantec Corporation

/s/ *John F. Horvath*
John F. Horvath

80034097.doc